Version Number: 01-2017

U.S. Department of Commerce
U.S. Census Bureau

Privacy Impact Assessment
for the
CEN05 Field Systems Major Application System

Reviewed by: _____, Bureau Chief Privacy Officer, Acting
Byron Crenshaw

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CATRINA PURVIS Digitally signed by CATRINA PURVIS Date: 2020.09.21 18:52:42 -04'00' 05/04/2020

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
U.S. Census Bureau/CEN05 Field Systems Major Application System

Unique Project Identifier: 006-000401400

Introduction: System Description

(a) Whether it is a general support system, major application, or other type of system

The CEN05 Field Systems Major Application System is a major information system managed by the Application Development Services Division (ADSD) in support of the Census Bureau Field Directorate.

(b) System location

The IT system is housed at the Census Bureau's Bowie, MD computer center. There are also components hosted in the Amazon Web Services (AWS) cloud, located in the Northeastern part of the United States.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

CEN05 interconnects with other IT systems. Desktop and laptop client services are provided by CEN17; server support is provided by CEN16; Oracle 12c database support is provided by CEN18, and; Decennial support is provided by CEN08 TI.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

The Field Directorate plans, organizes, coordinates, and carries out the Census Bureau's field data collection program for sample surveys, special censuses, the Economic Census, and the Decennial census. The CEN05 IT system maintains Personally Identifiable Information (PII) collected from respondents for these surveys and censuses such as name, address, contact information, race, gender, education, financial information, etc. In addition, Field Representative characteristics are also collected while surveys and census interviews are conducted.

Laptops are used to collect survey data in the field. An application assigns cases and monitors interviewing progress. Information systems covered by other CEN plans are used as routing mechanisms to transfer survey data from various survey sources, that includes but are not limited to, computer interviewing, telephone interviewing utilizing Census Bureau computer programs, internet self surveys, and paper surveys to the survey sponsors.

In addition to laptops, the Field Directorate has begun utilizing both tablet and other mobile computing devices to perform Census tests that lead up to the 2020 Decennial Census to collect respondent information using Census Bureau-issued mobile devices.

The Customer Experience Management (CEM) System is a centralized data store from five data sources currently being utilized by the Census Bureau and will deploy an enterprise dashboard for Census Bureau leadership.

This dashboard will provide insights into customer engagement for Census Bureau products & services, and will allow analysts to leverage data across data sources on a holistic Business Intelligence (BI) platform. The system will not only eliminate manual processes, but will:

1) Create an opportunity for a better understanding of patterns and trends of customer experiences that can lead to actionable improvement plans, and;
2) Establish a framework and foundation for other data integration, BI, and analytics efforts.

CEM will interface/collect information for various sources inside and outside of the Census Bureau and will contain PII data.

The Census Enterprise Data Collection and Processing initiative (CEDCaP) is a suite of IT systems and supporting infrastructure to handle data collection and processing for the nearly 100 surveys and three censuses conducted by the Census Bureau. CEN05 is part of this infrastructure and includes the *Enterprise Censuses and Surveys Enabling platform (ECaSE) which* will provide about half the data collection capabilities for CEDCaP

The ECaSE – ISR (Internet Self-Response) secure Internet data exchange system is a web-based framework for the design, delivery, and execution of surveys, censuses, and other data collection and data exchange efforts over the Internet. The enterprise-level application offers data collection areas the ability to reach a large number of potential respondents online, in a customizable manner to suit their business needs. ECaSE – ISR is developed to support increased demand for online data collections, including the extremely high loads associated with the 2020 Decennial Census.

ECaSE – OCS (Operational Control System) will serve as the standard tool to assign, control, track, and manage listing, survey and census workloads for the field workforce. ECaSE – OCS provides an enterprise application framework for this need, regardless of the interviewer-assisted mode used (phone or in person).

Enumeration is additional functionality given to the ECaSE to support respondents and the overall CEDCaP initiative. For Internet data capture, providing real-time edits, ability to capture household entries, and multi-access methods across different technologies (e.g., computers, phones, tablets, kiosks).

To establish a cohesive IT system boundary for the purposes of security assessment, the CEN05 IT system is comprised of three major areas: Collections, Business Support Processes, and Backend Processes. Each of these major components employs security control mechanisms that must be individually documented to ensure that the system as a whole is appropriately protected. As such, the system security plan is organized to reflect the implementation of technical controls for each subsystem component.

Application Development and Software Division (ADSD) incorporated a Survey Field Identification Tool (sFIT) to aid in investigating situations where it is suspected that a Field Representative (FR) may be falsifying respondent information. The tool will be used by Contact Center and Regional Office (RO) representatives to indicate FR who are suspected of falsification and to facilitate and document the results of the investigations. The newly developed tool replaced the previous automated system and the paper 11-163 forms. sFIT collects and disseminates PII regarding a survey respondent and the Field Representative who is suspected of falsifying survey data.

(e) How information in the system is retrieved by the user

There are many external sponsors, but CEN05 does not have direct connections to any of them. Demographics Survey Division (DSD), the Economics Directorate , etc., will give CEN05 the surveys that they have crafted for the external sponsors and the data collected for those surveys is placed into the CEN05 Master Control System (MCS) for the internal system to pick up. It will be the other internal sponsors' responsibility to vet the information, transform it into a format that the external sponsors can ingest and send it off. The sharing of the data should be on those systems with the external connection to the external sponsors. Individual or household records containing PII are retrieved by any number of personal identifiers collected including name, address, contact information, etc..

(f) How information is transmitted to and from the system

Data collected via CEDCAP and ECaSE is transmitted to the CEN05 IT secure data warehouse The Data warehouse extracts and provides a view of survey data over time, data collection modes, and data collection operations. It aggregates data and creates canned reports. These reports are made available to stakeholders, approved individuals, and organizations to support optimization and coordination of decennial, current, and special surveys. The reports are developed by a special staff that was established through the Office of the Director to serve as an analytic team with specific, ongoing responsibilities to develop analytic tools (charts and tables). These tools will be used by decennial and current survey field managers toward the goal of continuous improvement in survey operational efficiency. This group will both initiate and respond to issues related to survey performance indicators including cost, data quality, and data collection progress. This database interfaces with systems throughout the Census Bureau that contain PII, Business Identifiable Information (BII), and data collected and/or protected under Title 13 and Title 26.

(g) Any information sharing conducted by the system

The CEN05 IT system only shares PII and BII data within other CEN05 systems/components and with other Census Bureau IT systems in CEN03, CEN04 CBS, CEN06 NPC, CEN11, CEN13, CEN22, CEN35, and CEN36.

The data warehouse provides the ability for survey sponsors to view statistical data. It does not allow access to the information at the individual case level where the "raw" data resides. The data warehouse interacts with multiple systems within the Census Bureau network such as the system that contains information about businesses, which provides the mailing list for the Economic Census, and the primary sampling frame for virtually all other business surveys. The survey information about businesses is collected to track the movement of commodities from businesses throughout the United States. The data will be stored in its "raw" form and then transformed and stored in the data warehouse. The data warehouse will tabulate the data and display it in various reports. The data in its "raw" form will not be displayed. The data warehouse maintains PII, BII, Title 13 and Title 26 information.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

15 U.S.C. 301
13 U.S.C. Chapter 5, 6(c), 8(b), 131, 132, 141, 161, 182, 193, 196
15 CFR, Part 50.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Some added components are in the cloud					

___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	
b. Taxpayer ID		f. Driver's License		j. Financial Account	
c. Employer ID		g. Passport		k. Financial Transaction	
d. Employee ID	X	h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:

1) Employee's full SSN info needed for cost reimbursement and other financial purposes.
2) The last 4 digits of the survey respondent's SSN helps is collected on behalf of the survey sponsor, The National Center for Health Statistics (NCHS). The justification for the necessity of collecting this information, taken from the latest approved Office of Management and Budget (OMB) Information Collection Request (ICR) supporting statement is below:

Social Security Number and Health Insurance Claim Number: The last four digits of the Social Security Number (SSN) is asked on the NHIS questionnaire to allow linkage with administrative and vital records, such as the National Death Index (NDI). The NDI is a computerized central file of death record information. It is compiled from data obtained by NCHS from the State vital statistics offices. The data contain a standard set of identi-fying information on decedents from 1979 to the present. Records are matched using Social Security Number and other variables such as name, father's surname, date of birth, sex, state of resi-dence, and marital status. Of these, Social Security Number is the most important identifier for successful matching. The last four digits has been shown to be nearly as effective for matching as the full number.

The Social Security Number is also used by the Medical Expenditure Panel Study to help track the location of respondents who have changed residence since their NHIS interview. Finding a correct address for respondents is essential to maintaining response levels at an acceptable level in linked surveys, and the Social Security Number is a key item for establishing a correct address.

Medicare beneficiaries are given a health insurance claim (HIC) number that is their (or their spouse's) SSN with an alphabetic prefix. The NHIS also asks for the last four digits of that number so that the NHIS data can be linked to Medicare claims information for purposes of statistical research.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth	X	m. Religion	
b. Maiden Name	X	h. Place of Birth	X	n. Financial Information	X
c. Alias	X	i. Home Address	X	o. Medical Information	X
d. Gender	X	j. Telephone Number	X	p. Military Service	X
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education	X	r. Mother's Maiden Name	X
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title	X	e. Email Address	X	h. Work History	X
c. Work Address	X	f. Business Associates	X		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

CEN05 receives the information and passes the data to the internal sponsors. It is then the responsibility of the internal sponsors to vet the information and ensure it's accuracy before transforming it into a format that the external sponsors can ingest. The internal sponsors reside in different divisions/program areas within the Census Bureau, and then provide the data to their external sponsors via their program area IT systems (i.e. CEN18, CEN11, etc…).

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. For the Decennial Census survey, the OMB Number is 0607-1006 For the American Community Survey, the OMB Number is 0607-0810 For the Economic and Demographic surveys, the U.S. Census Bureau has obtained approval from OMB for the collection of survey information per each survey. Individual Paperwork Reduction Act control numbers are assigned to surveys with 10 or more respondents.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			
X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.		

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	X	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			
	There are not any IT system supported activities which raise privacy risks/concerns.		

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	X
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	

Other (specify): For statistical purposes

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

Census Bureau information shapes important policy and operational decisions that help improve the nation's social and economic conditions. We conduct the constitutionally mandated Census of Population and Housing every 10 years for all persons living in the U.S., which is used to apportion seats in the House of Representatives and informs congressional redistricting.

We also conduct a census of all business establishments and of all governmental units, known respectively as the Economic Census and the Census of Governments, every five years. The Economic Census is the benchmark used for measuring Gross Domestic Product (GDP) and other key indicators that guide public policy and business investment decisions.

In addition, we conduct several ongoing business and household surveys that provide the information in several of the Nation's key economic indicators and which is used to allocate over $400 billion in Federal funding annually.

The PII/BII collected for statistical purposes: The PII/BII maintained is from voluntary and mandatory surveys, census interviews, pilot tests and cognitive interviews collected from members of the public.

The PII collected for administrative purposes: We collect information about Census Bureau employees during the collection of respondent information. Field representative and interviewer characteristics obtained during census and survey interviews, pilot tests, and cognitive interviews are used for research and analytical studies to evaluate Census Bureau surveys and programs.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

The Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well.

All Bureau employees and contractors undergo mandatory annual data stewardship training to include proper handling, dissemination, and disposal of BII/PII/Title 13/Title 26 data.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.

	Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: CEN03, CEN04 CBS, CEN06 NPC, CEN11, CEN13, CEN22, CEN35, CEN36 CEN05 uses a multitude of security controls mandated by the Federal Information Security Management Act of 2002 (FISMA) and various other regulatory control frameworks including the National Institute of Standards and Technology (NIST) special publication 800 series. These security controls include, but are not limited to the use of mandatory HTTPS for public facing websites, access controls, anti-virus solutions, enterprise auditing/monitoring, encryption of data at rest, and various physical controls at the Census Bureau facilities that house Information Technology systems. The Census Bureau also deploys an enterprise Data Loss Protection (DLP) solution as well.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: http://www.census.gov/about/policies/privacy/privacy-policy.html	
X	Yes, notice is provided by other means.	Specify how: as specified in some survey instrument(s), respondent letters, etc.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For voluntary surveys or censuses, the respondent has an opportunity to decline to provide PII/BII.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For mandatory surveys or censuses, the respondent does not have an opportunity to decline to provide PII/BII

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their	Specify how: For Employee Productivity Measurement Records the consent is required for employment. Survey

	PII/BII.	respondents are notified via Privacy Act Statements/Introductory letters the purposes/use of collection of PII. By providing their information the respondent is consenting to uses described in Introductory letters/Privacy Act Statements.
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Respondents are notified via Privacy Act Statements/Introductory letters the purposes of collection of PII. For mandatory surveys/censuses, respondents do not have an opportunity to consent to uses.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: : As identified in the applicable SORN for Employee Productivity Measurement Records, these individual may contact the Associate Director for Field Operations for access to these records.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: As identified in the applicable SORNs Census-3, -4, -5, and -7 the records are exempted from notification, access, and contest requirements of the agency procedures (under via 5 U.S.C 552a(c)(3),(d), (e),(1), (e),(4),(G), (H) and (I), and (f). The data are maintained by the U.S. Census Bureau solely as statistical records as required under Title 13 U.S.C., and are not used in whole or in part in making any determination about an identifiable individual. This exemption is also made in accordance with the Department's rules which appear in 15 CFR part 4 subpart B.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: All systems are audited and monitored per U.S. Census Bureau Enterprise Audit procedures.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): __ECaSE: 3/13/2019. Field:

	7/9/2019_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
X	Other (specify): Publications are approved by the Disclosure Review Board

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The Census Bureau Information technology systems employ a multitude of layered security controls to protect BII/PII at rest, during processing, as well as in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Mandatory use of HTTP(S) for Census Bureau Public facing websites
- Use of trusted internet connection (TIC)
- Anti-Virus software to protect host/end user systems
- Encryption of databases (Data at rest)
- HSPD-12 Compliant PIV cards
- Access Controls

The Census bureau Information technology systems also follow the National Institute of Standards and Technology (NIST) standards including special publications 800-53, 800-63, 800-37 etc. Any system within the Census Bureau that contains, transmits, or processes BII/PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The Census Bureau also deploys a Data Loss Prevention solution as well.

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/CENSUS-2, Employee Productivity Measurement Records: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-2.html COMMERCE/CENSUS-3, Special Censuses, Surveys, and Other Studies: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-3.html COMMERCE/CENSUS-4, Economic Survey Collection: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-4.html COMMERCE/CENSUS-5, Decennial Census Program: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-5.html COMMERCE/CENSUS-7, Special Censuses of Population Conducted for State and Local Government: http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 3.1: General Technology Management Records; GRS 3.2: Information Systems Security Records; GRS 4.1: Records Management Records; GRS 4.2: Information Access and Protection Records; GRS 4.3: Input Records, Output Records, and Electronic Copies, N1-29-89-5 American Housing Survey, NC1-29-79-7 Demographic Fields Area, NC1-29-80-6 Demographic and Economic area Divisions - Secondary Use Sampling Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individual data elements directly identifying unique individuals.
X	Quantity of PII	Provide explanation: A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.
X	Data Field Sensitivity	Provide explanation: Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
X	Context of Use	Provide explanation: Disclosure of the PII is likely to result in severe or catastrophic harm to the individual or organization.
X	Obligation to Protect Confidentiality	Provide explanation: Organization or Mission- specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to government- wide or industry-specific requirements. Violations may result in severe civil or criminal penalties. PII in this IT system is collected under the authority of Title 5 and Title 13.
X	Access to and Location of PII	Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization- owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)).
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The biggest potential threat to privacy is the potential loss of a Field Representative's CAPI laptop. This threat is mitigated by the use of full disk encryption of the hard drive or solid state drive which renders the data inaccessible in the event that laptop is lost, damaged, or stolen. Due to the quantity, nature, and scope of the multiple surveys collected and processed through CEN05 (including the upcoming Decennial Census), there are no plans to reduce the quantity or type of data being collected, nor the sources of that data.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.